

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25

2
3
4
5

7

8

9
10
11
12

14

15

16

19

22

21
22
23

24

25

1 same stick with multiple vendors. The system is sound, in that the cost to break
2 the system exceeds the maximal possible theft due to the break.

3 The electronic asset system includes a bank B (or other type of issuer), a
4 user U , and multiple vendors $V1, V2, \dots, VM$. The system may also include an
5 auditor A , although the bank/issuer may perform the auditing functions. The
6 process has four phases: withdrawal, payment, deposit, and audit.

7 During the withdrawal phase, a user creates a stick of L electronic assets by
8 computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

12 where $h(x)$ is a hashing function of a value x . The user then forms a withdrawal
13 request having a user identity U , a user secret K , the bottom asset C_L taken from a
14 bottom of the stick, a denomination d indicating a value for the assets in the stick,
15 an expiration t , and the length L (i.e., number of assets in the stick). The user
16 submits the withdrawal request to the bank, which signs the withdrawal request:

$$S_B(U, K, d, C_L, t, L)$$

20 The bank returns the bank-signed withdrawal request to the user. The resulting
21 stick and signed withdrawal request are not dependent on, nor limited to any
22 vendor. Accordingly, the user is free to spend assets from the stick with different
23 vendors.

24 During the payment phases, the user decides to spend one or more assets
25 from the stick with a vendor having an identity V . The user forms a payment

1 request by concatenating the vendor identity V , a first asset C_j to be spent from the
2 stick, a depth D indicating a distance of the first asset from the bottom of the stick,
3 and a nonce (i.e., a random value generated by the user for inclusion in the
4 payment request). The user signs the payment request:

$$S_U(C_j, D, V, \text{nonce})$$

8 The user submits the signed payment request along with the bank-signed
9 withdrawal request to the vendor. The vendor evaluates the signatures of the bank
10 and user and ensures that the coin is properly contained within the stick. If all tests
11 pass, the vendor accepts the first asset as payment. Subsequent to this first asset,
12 the user can pass any additional assets from the stick as payment without digitally
13 signing them.

14 During the deposit phase, the vendor periodically creates a deposit request
15 having the user-signed first asset $S_U(C_j)$, a last asset spent from the stick C_k , and a
16 run length RL of assets beginning with the first asset C_j and ending with the last
17 asset C_k . The vendor signs the deposit request:

$$S_V(S_U(C_j), C_k, RL)$$

21 The vendor submits the vendor-signed deposit request along with the bank-
22 signed withdrawal request to the bank. The bank evaluates the vendor signature,
23 the user signature, and its own signature. The bank ensures that the assets are from
24 the stick and credits the vendor's account with the run of assets.

1 During the audit phase, the vendor wallet randomly selects samples of the
2 assets spent by the user and submits the samples to the auditor. The auditor checks
3 whether the assets have been used in a fraudulent manner (i.e. double spent coins).
4 If so, the user identity is revoked. The auditor also employs a deterministic audit
5 that evaluates all spent assets deposited with the bank for purposes of uncovering
6 fraud.

7 The electronic asset system employs tamper-resistant electronic wallets
8 embodied in a number of different ways, including smart cards, handheld
9 computing devices, and computers. The wallets are constructed as dedicated
10 hardware devices or as devices with secure-processor architecture. The breaking
11 cost of such wallets is higher than the amortized cost of printing or minting false
12 conventional cash. The claims capture this architecture and new technology.

13 **Claim 1** for example recites a method comprising:

14 minting a stick of electronic assets by digitally signing with an
15 issuer's signature a composite of user-provided data items including a user
16 identity, a bottom asset from a bottom of the stick, and a length of the stick;

17 spending one or more assets from the stick at one or more vendors,
18 wherein each expenditure with a particular vendor involves digitally signing
19 with a user's signature a first asset from the stick to be spent and passing
20 the user-signed first asset along with the issuer-signed composite to the
21 particular vendor for verification and subsequently passing any additional
22 assets to be spent without user signature to the particular vendor; and

23 depositing one or more assets collected by the particular vendor by
24 digitally signing with the particular vendor's signature a composite of data
25 items including the user-signed first asset and a last asset spent by the user

1 from the stick and passing the vendor-signed composite along with the
2 issuer-signed composite to the issuer.

3 The method of claim 1 is not disclosed by Briscoe. Briscoe shows a
4 transaction system for use by a broker for minting an electronic coin stick. A
5 client (user) initiates contact with a broker (banker) (Briscoe at col. 5 line 13, Fig.
6 2). The client requests that the broker issue a coin stick having a specific value,
7 and the client pays for the coin stick (Briscoe at col. 5 lines 19-23). Briscoe does
8 not disclose nor teach that a client is able to mint its own coin stick.

9 The digitally signed contract of the coin stick in Briscoe includes only coin
10 stick value; coin stick denomination; hash function; coin stick identifier "i" unique
11 within the broker; and an address of the broker's authorization interface (broker
12 URL). (Briscoe at col. 5, lines 43-49). The only identifier that is attached to the
13 coin stick in Briscoe is the coin stick identifier "i" that is unique within the broker
14 (i.e., only the broker is able to differentiate particular coin sticks based on the
15 identifier). The coin stick is issued without being signed with the broker's
16 signature.

17 A client in Briscoe requests or provides information to the broker for a coin
18 stick of specific value, and a specific denomination. (Briscoe col. 5, lines 19-21).
19 Coin stick value and denomination are two parts of the digitally signed contract.
20 Briscoe does not disclose nor teach that a client provide a client identity in minting
21 the coin stick. Briscoe in fact teaches that "the present invention preserves
22 anonymity" and provides an anonymous payment method (Briscoe at col. 5, 23-
23 25). Attaching a client identity to the coin stick would defeat the object of
24 preserving client anonymity taught in Briscoe.
25

1 With a purchased broker-minted coin stick, the client accesses the website
2 of the vendor and begins "spending" assets from the coin stick. This spending
3 involves the transaction module in the vendor calculating the total price of the
4 requested pages by the client and requesting a prepayment of the total price from
5 the client into the vendor payment interface. (Briscoe col. 6, lines 13-16). In the
6 transaction (spending) between client and vendor, Briscoe is silent as to signing a
7 first asset with the user's signature. The vendor in Briscoe does not perform a
8 verification of broker and client signatures, since whatever assets that are
9 presented to the vendor lack client and broker signatures.

10 In Briscoe, in order to complete a purchase transaction, the vendor connects
11 to the broker's URL, specifically the authorization interface of the broker's URL,
12 pass to the broker the vendor's callback URL and confirm the validity and value of
13 the client's coin stick with the broker (Briscoe at col. 6, lines 31-40). The vendor
14 does not sign whatever assets that are transferred from the client.

15 Claim 1 recites in part "minting a stick of electronic assets by digitally
16 signing with an issuer's signature a composite of user-provided data items
17 including a user identity." Briscoe does not disclose this aspect. Specifically,
18 Briscoe's methodology does not disclose (1) a user supplying the data items for
19 minting; and (2) having the issuer sign the user provided data items from the stick.
20 As discussed, the broker creates the stick and the only identifier that is shown in
21 Briscoe is a coin stick identifier which is unique only to the broker. The Examiner
22 has pointed out that Briscoe col. 5, lines 44-49 disclose digitally signing with an
23 issuer signature and providing user identity. The section identified by the
24 Examiner includes only the following items in the contract between broker and
25 user: the coin stick value, the coin stick denomination, the hash function, the coin

1 stick identifier, and the broker's authorization interface (URL). This section and
2 the rest of Briscoe are silent as to the requirement of the user supplying data items
3 for minting, and having the issuer sign the user provided data items from the stick.

4 Claim 1 recites in part "spending one or more assets from the stick at one or
5 more vendors, wherein each expenditure with a particular vendor involves digitally
6 signing with a user's signature a first asset from the stick to be spent and passing
7 the user-signed first asset along with the issuer-signed composite to the particular
8 vendor for verification and subsequently passing any additional assets to be spent
9 without user signature to the particular vendor." Briscoe does not disclose nor
10 teach that the use of a user signature, and in particular a user signature to sign a
11 first asset. As discussed, the issuer never signs the assets. Also as discussed, since
12 the vendor never receives assets signed by an issuer and a user, the vendor is not
13 able to perform verification of the assets based on an issuer-signed composite and
14 subsequent user signature of a first asset or data item. The Examiner asserts that
15 these requirements are found in Briscoe col. 1, lines 63-67 to col. 2 lines 1-24.
16 The section pointed out by the Examiner, as well as the rest of Briscoe, is silent as
17 to a user signature, an issuer signature, and verification of the vendor using user
18 and issuer signatures. Further, Briscoe does not disclose spending assets from the
19 stick with one or more vendors. Briscoe fails to disclose how the same stick could
20 be used with a second vendor. Briscoe would require a different stick to be minted
21 by a broker to be spent with a second vendor. In this respect, Briscoe is akin to the
22 architecture described in the background section of the subject application.

23 Claim 1 further recites "depositing one or more assets collected by the
24 particular vendor by digitally signing with the particular vendor's signature a
25 composite of data items including the user-signed first asset and a last asset spent

1 by the user from the stick and passing the vendor-signed composite along with the
2 issuer-signed composite to the issuer.” Briscoe does not disclose nor teach a
3 vendor collecting assets by digitally signing the assets with the vendor’s signature.
4 A vendor in Briscoe connects with the website of a broker and presents for
5 confirmation the coin stick with identifier “i” unique to the broker having a length
6 of Z_{m+n} (Briscoe col. 6, lines 35-36). Briscoe does not disclose nor teach that the
7 vendor is required to sign the assets that are collected. The Examiner points that
8 this requirement is disclosed in Briscoe col. 6, lines 21-46. This particular section
9 describes the user transacting with a specific vendor; the user calculating from the
10 stick a hash value that is presented and compared by the vendor; and the vendor
11 presenting to the issuer request for payment based on the calculated hash value.
12 This particular section and the rest of Briscoe, however, are silent as to the
13 requirement of a vendor signing assets.

14 For these reasons, claim 1 is patentable over Briscoe. Applicants
15 respectfully request that the §102 rejection of claim 1 be withdrawn.

16 **Dependent claims 2-5, 7-11** are allowable by virtue of their dependency on
17 base claim 1. For the reasons given above with respect to claim 1, the systems and
18 methods recited in claims 2-5, 7-11 are neither disclosed nor taught by Briscoe.
19 Applicants respectfully request that the §102 rejection of claim 2-5, 7-11 be
20 withdrawn.

21 **Claim 24** recites a method for issuing electronic assets, comprising:

22 creating, at a user, a stick of L electronic assets by computing:

23
24
$$C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

1 where $h(x)$ is a hashing function of a value x ;
2 submitting a withdrawal request from the user to an issuer, the
3 withdrawal request having a user identity U , a last asset value C_L taken from
4 a bottom of the stick, and the value L , while omitting any vendor identity;
5 signing, at the issuer, the withdrawal request; and
6 returning the signed withdrawal request to the user.

7 The method of claim 24 is not disclosed by Briscoe. Briscoe shows a
8 transaction system for use by a broker for minting an electronic coin stick. A
9 client (user) initiates contact with a broker (banker) (Briscoe at col. 5 line 13, Fig.
10 2). The client requests that the broker issue a coin stick having a specific value,
11 and the client pays for the coin stick (Briscoe at col. 5 lines 19-23). Briscoe does
12 not disclose nor teach that a client is able to mint its own coin stick

13 Briscoe fails to disclose "creating, at a user, a stick of L electronic assets"
14 as required by claim 24. Instead, Briscoe discloses that the broker creates the
15 stick. The Examiner points out that Briscoe Fig. 3, col. 3 lines 54-55 disclose
16 creating at a user a stick of L electronic assets. This section describes "generating
17 a hash chain of values which are derived from the secret number." This is
18 described as a method that is performed "at a first party ("the broker")" (Briscoe at
19 col. 3 line 48). This section and the rest of Briscoe fail to describe a user creating
20 the stick.

21 Briscoe does not disclose "submitting a withdrawal request from the user to
22 an issuer, the withdrawal request having a user identity" as recited by claim 24.
23 The Examiner points to Briscoe at col. 6, lines 21-46 as disclosing a user
24 submitting a withdrawal request from an issuer. This section describes the user
25 transacting with a specific vendor; the user calculating from the stick a hash value

1 that is presented and compared by the vendor; and the vendor presenting to the
2 issuer request for payment based on the calculated hash value. This particular
3 section does not discuss a client or user making a withdrawal request from a
4 broker. Furthermore, the Examiner is inconsistent in his positions. The Examiner
5 has referred to Briscoe at col. 6, lines 21-46 earlier as disclosing "depositing by a
6 vendor." This section as discussed above, describes the transaction between
7 vendor and issuer for the vendor to receive payment from the coin stick presented
8 by a client (user). Further, the rest of Briscoe does not disclose a user submitting a
9 withdrawal request with an issuer.

10 Briscoe further fails to disclose "signing, at the issuer, the withdrawal
11 request; and returning the signed withdrawal request to the user." The Examiner
12 points to Briscoe at col. 6, lines 21-46 as disclosing this requirement. As discussed
13 above, this section of Briscoe describes the user transacting with a specific vendor;
14 the user calculating from the stick a hash value that is presented and compared by
15 the vendor; and the vendor presenting to the issuer request for payment based on
16 the calculated hash value. This section and the rest of Briscoe fail to disclose an
17 issuer-signed withdrawal request that is returned to the user.

18 For these reasons, claim 24 is patentable over Briscoe. Applicants
19 respectfully request that the §102 rejection of claim 1 be withdrawn.

20 **Dependent claims 25-30** are allowable by virtue of their dependency on
21 base claim 24. For the reasons given above with respect to claim 1, the systems
22 and methods recited in claims 25-30 are neither disclosed nor taught by Briscoe.
23 Applicants respectfully request that the §102 rejection of claim 25-30 be
24 withdrawn.
25

1 **35 U.S.C. §103**

2 **Claims 4, 15, and 54** stand rejected under 35 U.S.C. §103(a) as being
3 unpatentable over Briscoe in view of U.S. Patent No. 5,878,140 to Chaum
4 (hereinafter “Chaum”). Applicants respectfully traverse the rejection.

5 **Claim 4** depends from claim 1 and hence incorporates the features of claim
6 1. As such claim 4 requires “minting a stick of electronic assets ... with an
7 issuer’s signature a composite of user-provided data items including a user identity
8 ...; spending one or more assets from the stick at one or more vendors, wherein
9 each expenditure with a particular vendor involves digitally signing with a user’s
10 signature a first asset from the stick to be spent and passing the user-signed first
11 asset along with the issuer-signed composite to the particular vendor for
12 verification and subsequently passing any additional assets to be spent without user
13 signature to the particular vendor; and depositing one or more assets collected by
14 the particular vendor by digitally signing with the particular vendor’s signature a
15 composite of data items including the user-signed first asset ... and passing the
16 vendor-signed composite along with the issuer-signed composite to the issuer.”

17 Briscoe does not suggest nor teach that a stick of electronic assets have an
18 issuer’s signature and a user’s signature (identity). The coin stick in Briscoe is
19 minted by a broker, and does not provide that a user identity or signature be
20 attached. Briscoe does not suggest nor teach that a vendor signature be attached to
21 assets presented to a broker. A vendor receives payment from a broker by
22 providing only the coin stick with identifier “i” that was created when the broker
23 minted the coin stick (Briscoe at col. 6, lines 35-38).

24 Chaum is cited for its teaching of a blind protocol. Chaum provides no
25 assistance in light of Briscoe as to the recited methodology of claim 4.

1 Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the
2 claimed methods. Applicants respectfully request that the §103 rejections of claim
3 4 be withdrawn.

4 **Claim 15** depends from claim 12 and hence incorporates the features of
5 claim 12. Since claim 15 depends, and incorporates the features of base claim 12,
6 Applicants, initially question whether the rejection of claim 15 over the
7 combination of Briscoe/Chaum is proper given the Examiner's separate rejection
8 of base claim 12 over a different combination of Briscoe and Official Notice.

9 In any event, since claim 15 depends from claim 12, claim 15 requires
10 "forming a stick of L electronic assets C_i (for $i=1, \dots, L$) where each asset can be
11 derived from a preceding asset in the stick; signing the stick with a signature of a
12 party issuing the assets; spending a first run of one or more assets from the stick at
13 a first vendor; and spending a second run of one or more assets from the stick at a
14 second vendor."

15 Briscoe does not suggest nor teach a party that forms a stick, sign the stick
16 with the party's (issuer) signature. Although Briscoe discloses an issuer providing
17 an identifier "i", the identifier "i" is unique to the broker and is only used to
18 identify the coin stick to the broker. The identifier "i" is not considered a broker
19 signature (Briscoe at col. 5, line 48). Further, although Briscoe shows a client and
20 vendor performing a transaction, Briscoe is silent as to spending a second run of
21 one or more assets from the stick with a second vendor.

22 Chaum is cited for its teaching of a blind protocol. Chaum provides no
23 assistance in light of Briscoe as to the recited methodology of claim 15.
24 Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the
25

1 claimed methods. Applicants respectfully request that the §103 rejections of
2 claims 15 be withdrawn.

3 **Claim 54** depends from claim 51 and hence incorporates the features of
4 claim 51. Since claim 54 depends and incorporates the features of base claim 51,
5 Applicants question the Examiner's rejection of claim 51 over the combination of
6 Briscoe/Chaum, and Examiner's separate rejection of base claim 51 over a
7 combination of Briscoe and Schneier.

8 **Claim 54** depends from claim 51 and hence incorporates the features of
9 claim 51. As such claim 54 requires an issuer wallet with an issuer's signature a
10 composite of user-provided data items including a user identity; a user wallet to
11 store the stick of electronic assets, the user wallet spending one or more assets by
12 signing with a user's signature a first asset to be spent and passing the asset along
13 with the issuer-signed composite to the vendor for verification; whereupon
14 verification, the user wallet subsequently passes any additional assets to be spent
15 without user signature to the vendor; and a vendor wallet having to store one or
16 more assets spent by the user wallet, the vendor wallet depositing the assets
17 collected from the user wallet by signing with the particular vendor's signature a
18 composite of data items including the user-signed asset passed in the stick received
19 from the user wallet and passing the vendor-signed composite along with the
20 issuer-signed composite to the issuer wallet for verification.

21 Briscoe does not suggest nor teach the use of three separate wallets, an
22 issuer, a user, and a vendor (Briscoe col. 7, lines 57-63). Briscoe shows a smart
23 card that may be used as a hardware wallet for a user; however, Briscoe is silent as
24 to the use of a smart card for a vendor or an issuer. As discussed above, Briscoe
25

1 does not suggest nor teach the use of signatures of a user, a broker, and vendor.
2 Without signatures of the parties involved, security may be compromised.

3 Chaum is cited for its teaching of a blind protocol. Chaum provides no
4 assistance in light of Briscoe as to the recited methodology of claim 54.
5 Accordingly, a combination of Briscoe and Chaum fails to teach or suggest the
6 claimed methods. Applicants respectfully request that the §103 rejections of
7 claims 54 be withdrawn.

8 **Claim 5** stands rejected under 35 U.S.C. §103(a) as being unpatentable over
9 Briscoe in view of Official Notice.

10 **Claim 5** depends from claim 1 and hence incorporates the features of claim
11 1. As such claim 5 requires “minting a stick of electronic assets ... with an
12 issuer’s signature a composite of user-provided data items including a user identity
13 ...; spending one or more assets from the stick at one or more vendors, wherein
14 each expenditure with a particular vendor involves digitally signing with a user’s
15 signature a first asset from the stick to be spent and passing the user-signed first
16 asset along with the issuer-signed composite to the particular vendor for
17 verification and subsequently passing any additional assets to be spent without user
18 signature to the particular vendor; and depositing one or more assets collected by
19 the particular vendor by digitally signing with the particular vendor’s signature a
20 composite of data items including the user-signed first asset ... and passing the
21 vendor-signed composite along with the issuer-signed composite to the issuer.”

22 Applicants assert the arguments made in support of claim 4 above in respect
23 to the requirements outlined by base claim 1.

24 Official notice is taken that “signing the payment request with a signature of
25 the user” is common and well known in the prior art in reference to electronic

1 money. Applicants traverse such an assertion and request that the Examiner cite a
2 reference in support of his position. If the rejection is based on facts within the
3 personal knowledge of the Examiner, Applicants request an affidavit as provided
4 in MPEP § 2144.03. Nevertheless, the Official Notice taken provides no
5 assistance in light of Briscoe as to the recited methodology of claim 5.
6 Accordingly, a combination of Briscoe and the Official Notice taken fails to teach
7 or suggest the claimed methods. Applicants respectfully request that the §103
8 rejections of claims 5 be withdrawn.

9 **Claims 7, 8, 9, 19 and 20** stand rejected under 35 U.S.C. §103(a) as being
10 unpatentable over Briscoe in view of U.S. Patent No. 5,878,138 to Yacobi
11 (hereinafter "Yacobi"). Applicants respectfully traverse the rejection.

12 **Claims 7, 8, and 9** depend from claim 1 and hence incorporates the features
13 of claim 1. As such claims 7, 8, and 9 require "minting a stick of electronic assets
14 ... with an issuer's signature a composite of user-provided data items including a
15 user identity ...; spending one or more assets from the stick at one or more
16 vendors, wherein each expenditure with a particular vendor involves digitally
17 signing with a user's signature a first asset from the stick to be spent and passing
18 the user-signed first asset along with the issuer-signed composite to the particular
19 vendor for verification and subsequently passing any additional assets to be spent
20 without user signature to the particular vendor; and depositing one or more assets
21 collected by the particular vendor by digitally signing with the particular vendor's
22 signature a composite of data items including the user-signed first asset ... and
23 passing the vendor-signed composite along with the issuer-signed composite to the
24 issuer."
25

1 Applicants assert the arguments made in support of claim 4 above in respect
2 to the requirements outlined by base claim 1.

3 Yacobi is cited for its teaching of auditing the assets from the first and
4 second runs of assets for fraud. Yacobi provides no assistance in light of Briscoe
5 as to the recited methodology of claims 7, 8, and 9. Accordingly, a combination of
6 Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants
7 respectfully request that the §103 rejections of claims 7, 8, and 9 be withdrawn.

8 **Claims 19 and 20** depend from claim 12 and hence incorporate the features
9 of claim 12. As such claims 19 and 20 require “forming a stick of L electronic
10 assets C_i (for $i=1, \dots, L$) where each asset can be derived from a preceding asset in
11 the stick; signing the stick with a signature of a party issuing the assets; spending a
12 first run of one or more assets from the stick at a first vendor; and spending a
13 second run of one or more assets from the stick at a second vendor.”

14 Applicants assert the arguments made in support of claim 15 above in
15 respect to the requirements outlined by base claim 12.

16 Yacobi is cited for its teaching of auditing the assets from the first and
17 second runs of assets for fraud. Yacobi provides no assistance in light of Briscoe
18 as to the recited methodology of claims 19 and 20. Accordingly, a combination of
19 Briscoe and Chaum fails to teach or suggest the claimed methods. Applicants
20 respectfully request that the §103 rejections of claims 19 and 20 be withdrawn.

21 Claims 12, 13, 14, 16, 18, 21, 22, and 23 stand rejected under 35 U.S.C.
22 §103(a) as being unpatentable over Briscoe in view of Official Notice. Applicants
23 respectfully traverse the rejection.

24 **Claims 13, 14, 16, 18, 21, 22, and 23** depend from **claim 12** and hence
25 incorporate the features of claim 12. Claim 12 requires “forming a stick of L

1 electronic assets C_i (for $i=1, \dots, L$) where each asset can be derived from a
2 preceding asset in the stick; signing the stick with a signature of a party issuing the
3 assets; spending a first run of one or more assets from the stick at a first vendor;
4 and spending a second run of one or more assets from the stick at a second
5 vendor.”

6 As discussed above in support of claim 15, Briscoe does not suggest nor
7 teach a party that forms a stick, sign the stick with the party’s (issuer) signature.
8 Although Briscoe discloses an issuer providing an identifier “i”, the identifier “i”
9 is unique to the broker and is only used to identify the coin stick to the broker. The
10 identifier “i” is not considered a broker signature. Briscoe at col. 5, line 48.
11 Further, although Briscoe shows a client and vendor performing a transaction,
12 Briscoe is silent as to spending a second run of one or more assets from the stick
13 with a second vendor.

14 Official notice is taken that “spending a second run of one or more assets
15 from the stick at a second vendor”; “signing the payment request with a signature
16 of the user”; and “depositing the first and second runs of assets” is common and
17 well known in the prior art in reference to electronic money.

18 Applicants traverse the assertion of Examiner’s Official Notice that
19 “spending a second run of one or more assets from the stick at a second vendor” is
20 “well-known” prior art. Further, Applicants traverse that common knowledge in
21 the art would have shown the requirement can be combined with the other
22 requirements of “signing the payment request with a signature of the user”; and
23 “depositing the first and second runs of assets.” The background section of the
24 subject application explains that previous systems assign a single coin stick to a
25 single vendor, limiting the user to conduct transactions with only that vendor.

1 Applicants' system sought to alleviate this limitation of previous systems.
2 Therefore, contrary to the Office's position, it was not well known in the prior art
3 to spend assets from the same stick at multiple vendors. If a user desires to
4 transact with a second vendor, the user must contact the broker (issuer) to issue a
5 new stick that identifies the second vendor. If the Office maintains the rejection,
6 Applicants request that the Examiner cite a reference in support of this position. If
7 the rejection is based on facts within the personal knowledge of the Examiner,
8 Applicants request an affidavit as provided in MPEP § 2144.03. Nevertheless, the
9 Official Notice taken provides no assistance in light of Briscoe as to the recited
10 methodology of claim 12, 13, 14, 16, 18, 21, 22, and 23. Accordingly, a
11 combination of Briscoe and the Official Notice taken fails to teach or suggest the
12 claimed methods. Applicants respectfully request that the §103 rejections of
13 claims 12, 13, 14, 16, 18, 21, 22, and 23 be withdrawn.

14 Claims 51-53 stand rejected under 35 U.S.C. §103(a) as being unpatentable
15 over Briscoe in view of "Applied Cryptography" by Schneier (hereinafter
16 "Schneier"). Applicants respectfully traverse the rejection.

17 **Claims 52-53** depend from **claim 51** and hence incorporate the features of
18 claim 51. Claim 51 requires an issuer wallet having a with an issuer's signature a
19 composite of user-provided data items including a user identity; a user wallet to
20 store the stick of electronic assets, the user wallet spending one or more assets by
21 signing with a user's signature a first asset to be spent and passing the asset along
22 with the issuer-signed composite to the vendor for verification; whereupon
23 verification, the user wallet subsequently passes any additional assets to be spent
24 without user signature to the vendor; and a vendor wallet having to store one or
25 more assets spent by the user wallet, the vendor wallet depositing the assets

1 collected from the user wallet by signing with the particular vendor's signature a
2 composite of data items including the user-signed asset passed in the stick received
3 from the user wallet and passing the vendor-signed composite along with the
4 issuer-signed composite to the issuer wallet for verification.

5 Applicants assert the arguments made in support of claim 54 above in
6 respect to the requirements outlined by base claim 51.

7 Schneier is cited for its teaching of message transmission in order to prevent
8 adversaries from forging electronic asset transactions. Schneier provides no
9 assistance in light of Briscoe as to the recited methodology of claims 51-53.
10 Accordingly, a combination of Briscoe and Schneier fails to teach or suggest the
11 claimed methods. Applicants respectfully request that the §103 rejections of
12 claims 51-53 be withdrawn.

13 Claims 55-56 stand rejected under 35 U.S.C. §103(a) as being unpatentable
14 over Briscoe in view of U.S. Patent No. 6,021,399 to Deemers et al (hereinafter
15 "Deemers"). Applicants respectfully traverse the rejection.

16 **Claims 55-56** depend from **claim 51** and hence incorporate the features of
17 claim 51.

18 Applicants assert the arguments made in support of claim 54 above in
19 respect to the requirements outlined by base claim 51.

20 Deemers is cited for its teaching of "an auditing system to audit the
21 electronic assets to detect whether assets have been used in a fraudulent manner"
22 and "a probabilistic auditing system to sample a subset of less than all electronic
23 assets, to detect whether assets have been used in a fraudulent manner." Deemers
24 provides no assistance in light of Briscoe as to the recited methodology of claims
25 55-56. Accordingly, a combination of Briscoe and Deemers fails to teach or

1 suggest the claimed methods. Applicants respectfully request that the §103
2 rejections of claims 55-56 be withdrawn.

3 Claims 59-60 stand rejected under 35 U.S.C. §103(a) as being unpatentable
4 over Briscoe in view of Yacobi. Applicants respectfully traverse the rejection.

5 **Claim 60** depends from **claim 59** and hence incorporates the features of
6 claim 59. Claim 59 requires an electronic wallet having memory and a processor,
7 the electronic wallet being programmed to: receive a run of assets from a user;
8 select a subset of less than all of the assets received from the user; and submit the
9 subset of assets to an auditor for evaluation of fraudulent expenditure.”

10 Examiner admits that Briscoe does not disclose an electronic wallet to
11 receive a run of assets from a user, select a subset of less than all of the assets
12 received from the user; and submit the subset of assets to an auditor for evaluation
13 of fraudulent expenditure.

14 Yacobi is cited for its teaching of “an electronic wallet to receive a run of
15 assets from a user, select a subset of less than all of the assets received from the
16 user; and submit the subset of assets to an auditor for evaluation of fraudulent
17 expenditure”; however, Examiner has not particularly pointed out an electronic
18 wallet in Yacobi that receives a run of assets. Examiner further has not
19 particularly pointed out in Yacobi where a subset of assets are presented to an
20 auditor for fraudulent expenditure. Accordingly, a combination of Briscoe and
21 Yacobi fails to teach or suggest the claimed methods. Applicants respectfully
22 request that the §103 rejections of claims 59 and 60 be withdrawn.

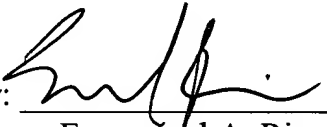
23 **Claim 60** which depends on claim 59 further recites in part “further
24 programmed to randomly select the subset of assets.”
25

1 CONCLUSION

2 All pending claims 1-41, 51-60 are in condition for allowance. Applicant
3 respectfully requests reconsideration and prompt issuance of the subject
4 application. If any issues remain that prevent issuance of this application, the
5 Examiner is urged to contact the undersigned attorney before issuing a subsequent
6 Action.

7
8
9 Date: 11/19/02

Respectfully Submitted,

10 By: 
11 Emmanuel A. Rivera
12 Reg. No. 45,760
13 (509) 324-9256 ext. 245
14
15
16
17
18
19
20
21
22
23
24
25

1 **MARKED UP VERSION OF PENDING CLAIMS UNDER 37 C.F.R. 1.121(C)(1)(ii):**

2 Amend claims 6, 17, and 58 as follows and in accordance with 37 C.F.R.
3 1.121(c)(1)(ii), by which the Applicant submits the following marked up version
4 only for claims being changed by the current amendment, wherein the markings
5 are shown by brackets (for deleted matter) and/or underlining (for added matter):
6

7 6. (Amended Once) A method [as recited in claim 1] comprising:
8 minting a stick of electronic assets by digitally signing with an issuer's
9 signature a composite of user-provided data items including a user identity, a
10 bottom asset from a bottom of the stick, and a length of the stick;

11 spending one or more assets from the stick at one or more vendors, wherein
12 each expenditure with a particular vendor involves digitally signing with a user's
13 signature a first asset from the stick to be spent and passing the user-signed first
14 asset along with the issuer-signed composite to the particular vendor for
15 verification and subsequently passing any additional assets to be spent without user
16 signature to the particular vendor; and

17 depositing one or more assets collected by the particular vendor by digitally
18 signing with the particular vendor's signature a composite of data items including
19 the user-signed first asset and a last asset spent by the user from the stick and
20 passing the vendor-signed composite along with the issuer-signed composite to the
21 issuer, wherein the depositing comprises:

22 concatenating the user-signed first asset $S_U(C_j)$, a last asset spent from the
23 stick C_k , and a run length RL of assets beginning with the first asset C_j and ending
24 with the last asset C_k to form a deposit request;

25 signing the deposit request with a signature of the vendor;

$$S_V(S_U(C_j), C_k, RL)$$

submitting the vendor-signed deposit request along with the issuer-signed withdrawal request to the issuer; and

crediting a vendor account with the run of assets in an event that the user, the vendor, the run, and the issuer are positively verified.

17. (Amended Once) A method [as recited by claim 16] for issuing electronic assets, comprising:

forming a stick of L electronic assets C_i (for $i=1, \dots, L$) where each asset can be derived from a preceding asset in the stick; wherein the forming [further] comprises:

creating the stick of L electronic assets by computing:

$$C_i = h^i(x) \text{ (for } i=1, \dots, L)$$

where $h(x)$ is a one-way hashing function of a value x ;

constructing a withdrawal request having a user identity U , a user secret K , a last asset value C_L taken from a bottom of the stick, a denomination d indicating a value for the assets in the stick, an expiration t ; and the value L ; and

signing the withdrawal request with a signature of an issuer:

$$S_I(U, K, d, C_L, t, L)[.];$$

1
2 signing the stick with a signature of a party issuing the assets;

3 spending a first run of one or more assets from the stick at a first vendor;

4 and

5 spending a second run of one or more assets from the stick at a second
6 vendor.

7
8 58. An electronic wallet [as recited in claim 57, further] having memory
9 and a processor, the electronic wallet being programmed to:

10 create a stick of L electronic assets by computing:

11
12
$$C_i = h^i(x) \quad (\text{for } i=1, \dots, L)$$

13
14 where $h(x)$ is a hashing function of a value x ;

15 form a withdrawal request having a user identity U , a last asset value C_L
16 taken from a bottom of the stick, and the value L , while omitting any vendor
17 identity;

18 submit withdrawal request to an issuer and receive the withdrawal request
19 back with an issuer signature;

20 store the signed withdrawal request and the stick;

21 form a payment request for payment of one or more assets from the stick to
22 a vendor having an identity V , the payment request having the vendor identity V
23 and a first asset C_j to be spent from the stick;

24 sign the payment request:
25

$S_U(C_j, VI)$; and

submit the signed payment request along with the signed withdrawal request to the vendor.



MARKED UP VERSION OF SPECIFICATION UNDER 37 C.F.R. §

1.121(B)(1)(iii):

Page 18, third paragraph

At step 102, the vendor sends the signed deposit request along with the signed withdrawal request to the [vendor]bank.

Page 26, fourth paragraph

Fig. 7 shows the linked dual-stick data structure 200 having a user stick 202 and a vendor stick 204. Each stick is configured according to a FIFO (first in first out) policy, where earned coupons are added to the top of the stick and spent coupons are removed from the bottom of the stick. Each stick has two pointers: a top pointer P_t and a bottom pointer P_b . As coupons are added, the top pointer P_t is incremented to reflect new coupons that are now available for use. As coupons are spent, the bottom pointer P_b is incremented to reflect their expenditure and reference the next unused coupon in the stick to be spent. The balance of available coupons, B , is equal to the difference between the top and bottom pointers (i.e., $B = P_t - P_b$).



DRAWINGS UNDER 37 C.F.R. § 1.121(D)

Drawing changes are submitted for Fig. 5, and are provided separately.

RECEIVED
NOV 22 2002
GROUP 3600